

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-224896

(43)Date of publication of application : 12.08.1994

(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G09C 1/00

(21)Application number : 05-303773

(71)Applicant : HITACHI LTD
HITACHI CHUBU SOFTWARE LTD

(22)Date of filing : 03.12.1993

(72)Inventor : MATSUMOTO HIROSHI
TAKARAGI KAZUO
SUZAKI SEIICHI
MAEZAWA HIROYUKI
KOIZUMI SHINOBU

(30)Priority

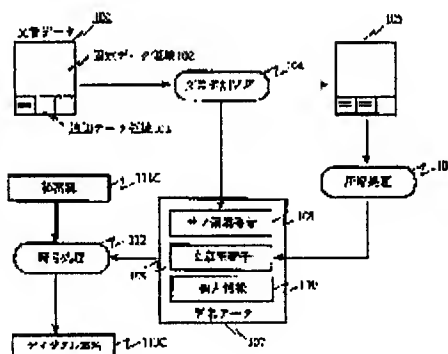
Priority number : 04350461 Priority date : 03.12.1992 Priority country : JP

(54) ELECTRONIC DOCUMENT PROCESSING SYSTEM AND PREPARING METHOD FOR DIGITAL SIGNATURE

(57)Abstract:

PURPOSE: To provide the preparing method for digital signature and an authentication method for electronic document so as to change document contents on the way of circulation.

CONSTITUTION: When a user adds or changes received document contents at a terminal equipment 10 receiving the electronic document to which the digital signature is added, signature data 107 containing version management information 108 required for restoring an electronic document 101 of a previous version from an electronic document 105 of a new version are processed in ciphering by a secret key 111 of the user so as to prepare the digital signature 113 of the user. Since the document provided with the version preceded by one version from the received document is restored by using version management information 208 contained in signature data 207 obtained by decoding the last digital signature by a public key 208, at the terminal equipment receiving the electronic document, the relation of correspondence between all the digital signatures and documents can be confirmed by the similar procedure.



LEGAL STATUS

[Date of request for examination] 05.04.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3260524

[Date of registration] 14.12.2001

[Number of appeal against examiner's decision of

rejection]

[Date of requesting appeal against examiner's decision of
rejection]

[Date of extinction of right]

14.12.2004

(19)日本国特許庁(J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平6-224896

(43)公開日 平成 6 年(1994) 8 月12日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00 9/10 9/12 G 0 9 C 1/00		8837-5L 7117-5K	H 0 4 L 9/ 00 審査請求 未請求 請求項の数18	Z O L (全 22 頁)
(21)出願番号	特願平5-303773	(71)出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目 6 番地	
(22)出願日	平成 5 年(1993)12月 3 日	(71)出願人	000233457 日立中部ソフトウェア株式会社 愛知県名古屋市中区栄 3 丁目10番22号	
(31)優先権主張番号	特願平4-350461	(72)発明者	松本 浩 愛知県名古屋市中区栄三丁目10番22号 日 立中部ソフトウェア 株式会社内	
(32)優先日	平 4 (1992)12月 3 日	(72)発明者	宝木 和夫 神奈川県川崎市麻生区王禅寺1099番地 株 式会社日立製作所システム開発研究所内	
(33)優先権主張国	日本 (J P)	(74)代理人	弁理士 小川 勝男	最終頁に続く

(54)【発明の名称】 電子化文書処理システムおよびデジタル署名の生成方法

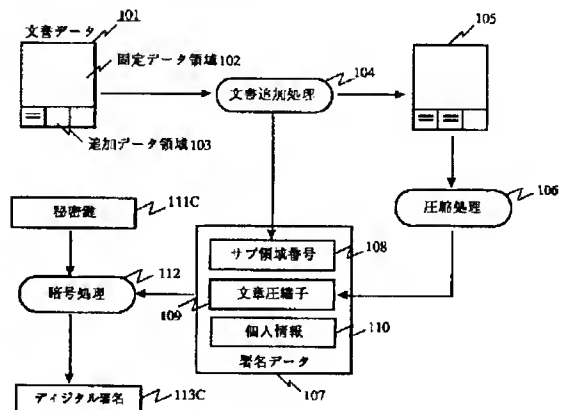
(57)【要約】

【目的】 回覧途中で文書内容の変更を可能にしたデジタル署名の生成方法と電子化文書の認証方法を提供する。

【構成】 デジタル署名が付された電子化文書を受け取った端末装置 1 0 で、ユーザが受信文書内容に追記または変更を行なった場合に、新バージョンの電子化文書 1 0 5 から前バージョンの電子化文書 1 0 1 を復元するために必要なバージョン管理情報 1 0 8 を含む署名データ 1 0 7 をユーザの秘密鍵 1 1 1 で暗号化処理することによって、上記ユーザのデジタル署名 1 1 3 を生成する。

【効果】 電子化文書を受信した端末装置では、最後のデジタル署名を公開鍵 2 1 1 で復号化して得られた署名データ 2 0 7 に含まれるバージョン管理情報 2 0 8 を用いて、受信文書から 1 つ前のバージョンをもつ文書を復元できるため、同様の手順で、全てのデジタル署名について文書との対応関係を確認できる。

図 1



【特許請求の範囲】

【請求項1】少なくとも1つのデジタル署名が関係付けられている前バージョンの電子化文書について、文書データの追記または変更を行なって新バージョンの電子化文書を作成し、

上記新バージョンの電子化文書を圧縮処理して文書の圧縮子を生成し、

上記文書圧縮子と、署名者の個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とを含む署名データを暗号化処理して、新たなデジタル署名を生成し、

上記新バージョンの電子化文書に、上記前バージョンの電子化文書に関係付けられていたデジタル署名と上記新たなデジタル署名とを関係付けることを特徴とするデジタル署名の生成方法。

【請求項2】前記署名データの暗号化処理が、公開鍵暗号化法において前記署名者に割り当てられた秘密鍵を用いて行われることを特徴とする請求項1に記載のデジタル署名の生成方法。

【請求項3】前バージョンの電子化文書が、データを追記するために用意された予め定義された複数の部分領域を有し、前記新バージョンの電子化文書が、前バージョンの電子化文書中の上記部分領域の1つに文書データを新たに追記することによって生成され、前記バージョン管理情報は、文書データが新たに追記された上記部分領域の1つを特定するための情報からなることを特徴とする請求項1に記載のデジタル署名の生成方法。

【請求項4】前記文書圧縮子が、前記新バージョンの電子化文書中の前記複数の部分領域に含まれる文書データを圧縮処理して得られる第1の圧縮子と、前記新バージョンの電子化文書中のその他の領域に含まれる文書データを圧縮処理して得られる第2の圧縮子とからなることを特徴とする請求項3に記載のデジタル署名の生成方法。

【請求項5】前記新バージョンの電子化文書が、前バージョンの電子化文書中の少なくとも1つの部分領域での新文書データの挿入または既存文書データの削除を行うことによって生成され、前記バージョン管理情報が、上記部分領域の位置と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなることを特徴とする請求項1に記載のデジタル署名の生成方法。

【請求項6】少なくとも1つのデジタル署名が関係付けられている前バージョンの電子化文書について文書データの追記または変更を行ない、新バージョンの電子化文書を作成し、

上記新バージョンの電子化文書を圧縮処理して第1の圧縮子を生成し、

上記新バージョンの電子化文書から上記前バージョンの

電子化文書を復元するために必要なバージョン管理情報を圧縮処理して第2の圧縮子を生成し、

上記第1の圧縮子と、上記第2の圧縮子と、署名者の個人情報とを含む署名データを暗号化処理して新たなデジタル署名を生成し、

上記新バージョンの電子化文書に、上記バージョン管理情報と、上記前バージョンの電子化文書に関係付けられていたデジタル署名と、上記新たなデジタル署名とを関係付けることを特徴とする電子化文書に付すべきデジタル署名の生成方法。

【請求項7】前記署名データの暗号化処理が、公開鍵暗号化法において前記署名者に割り当てられた秘密鍵を用いて行われることを特徴とする請求項6に記載の電子化文書に付すべきデジタル署名の生成方法。

【請求項8】前記新バージョンの電子化文書が、前バージョンの電子化文書中の少なくとも1つの部分領域での新文書データの挿入または既存文書データの削除を行うことによって生成され、前記バージョン管理情報が、上記部分領域の位置と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなることを特徴とする請求項6に記載の電子化文書に付すべきデジタル署名の生成方法。

【請求項9】前記新バージョンの電子化文書と対をなして複数のレコードからなるテーブルを有し、上記テーブルの各レコードが、各署名者の識別子と、前記バージョン管理情報と前記各デジタル署名の少なくとも一方を記憶することを特徴とする請求項8に記載の電子化文書に付すべきデジタル署名の生成方法。

【請求項10】所定の順序で付された複数のデジタル署名を伴う電子化文書の認証方法において、上記デジタル署名のうちの少なくとも1つが、署名者の個人情報と、該デジタル署名と対応するバージョンの電子化文書を圧縮処理して得られた圧縮子と、該デジタル署名と対応するバージョンの電子化文書から前バージョンの電子化文書を復元するために必要なバージョン管理情報とを含む署名データを暗号化して得たものであり、

(a) 上記受信メッセージに含まれる電子化文書をチェック対象文書として、チェック対象文書に所定の圧縮処理を施して圧縮子を生成し、

(b) 上記受信メッセージに含まれるデジタル署名のうち最新のものから順にチェック対象として選び、チェック対象となったデジタル署名の署名者と対応する復号鍵を用いて、該チェック対象デジタル署名から署名データを復号し、 (c) 上記復号された署名データから抽出された圧縮子と、上記チェック対象文書の圧縮子とが一致するか否かを検査し、

(d) 上記復号された署名データがバージョン管理情報を含む場合、該バージョン管理情報と上記チェック対象

文書とから、前バージョンの電子化文書を復元し、上記前バージョンの電子化文書と次のデジタル署名をそれぞれ新たなチェック対象文書およびチェック対象デジタル署名として、ステップ（a）～（c）を繰り返し、もし、上記復号された署名データがバージョン管理情報を含まない場合は、次のデジタル署名をチェック対象デジタル署名としてステップ（b）～（c）を繰り返すことを特徴とする電子化文書の認証方法。

【請求項11】前記ステップ（b）で行う前記署名データの復号を、公開鍵暗号法における前記署名者に対応する公開鍵を用いて行うことを特徴とする請求項10に記載の電子化文書の認証方法。

【請求項12】前記ステップ（d）で行う前記前バージョンの電子化文書の復元を、前記チェック対象文書から、前記バージョン管理情報が特定する部分領域の文書情報を削除することによって行うことを特徴とする請求項10に記載の電子化文書の認証方法。

【請求項13】所定の順序で付された複数のデジタル署名と、1つのバージョンの電子化文書から前バージョンの電子化文書を復元するために必要なバージョン管理情報とを伴う電子化文書の認証方法において、上記デジタル署名のうちの少なくとも1つが、署名者の個人情報と、該デジタル署名と対応するバージョンの電子化文書を圧縮処理して得られた第1の圧縮子と、該デジタル署名と対応するバージョン管理情報を圧縮処理して得られた第2の圧縮子とを含む署名データを暗号化して得たものであり、

（a）上記受信メッセージに含まれる電子化文書をチェック対象文書として、該チェック対象文書に所定の圧縮処理を施して圧縮子を生成し、

（b）上記受信メッセージに含まれるデジタル署名を最新のものから順にチェック対象として選び、チェック対象となったデジタル署名の署名者に対応する復号鍵を用いて、該チェック対象デジタル署名から署名データを復号し、

（c）上記復号された署名データから抽出された第1の圧縮子と、上記チェック対象文書の圧縮子とが一致するか否かを検査し、

（d）上記復号された署名データが第2の圧縮子を含む場合、上記受信メッセージに含まれるバージョン管理情報を最新のものから順にチェック対象管理情報として選び、該チェック対象管理情報に所定の圧縮処理を施して得られた圧縮子と上記第2の圧縮子とが一致するか否かを検査し、

（e）上記復号された署名データが第2の圧縮子を含む場合、上記チェック対象となったバージョン管理情報と上記チェック対象文書とから、前バージョンの電子化文書を復元し、上記前バージョンの電子化文書と次のデジタル署名をそれぞれ新たなチェック対象文書およびチェック対象デジタル署名として、ステップ（a）～

（d）を繰り返し、もし、上記復号された署名データがバージョン管理情報を含まない場合は、次のデジタル署名をチェック対象デジタル署名としてステップ

（b）～（d）を繰り返すことを特徴とする電子化文書の認証方法。

【請求項14】前記ステップ（b）で行う前記署名データの復号に、公開鍵暗号法における前記署名者に対応する公開鍵を用いることを特徴とする請求項10に記載の電子化文書の認証方法。

【請求項15】少なくとも1つのデジタル署名と前バージョンの電子化文書とを含む通信メッセージをネットワークから受信するための手段と、

上記ネットワークから受信した前バージョンの電子化文書とそれに付されたデジタル署名との関係をチェックするための検査手段と、

ユーザからの入力操作に応じて、上記前バージョンの電子化文書に部分的な変更または情報追加を行い、新バージョンの電子化文書を生成するための手段と、

上記新バージョンの電子化文書と所定の関係をもつ新たなデジタル署名を生成するための手段と、

上記新バージョンの電子化文書と、前バージョンの電子化文書と共に受信したデジタル署名と、上記新たなデジタル署名とを含む通信メッセージを上記ネットワークに送信するための手段とを有し、

上記デジタル署名生成手段が、上記新バージョンの電子化文書を圧縮処理して得られた文書圧縮子と、上記ユーザの個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とからなる署名データを、上記ユーザの秘密鍵で暗号化処理することによって、上記新たなデジタル署名を生成することを特徴とする電子化文書の処理システム。

【請求項16】前記検査手段が、

上記受信メッセージに含まれる電子化文書をチェック対象文書として、該チェック対象文書に所定の圧縮処理を施して文書圧縮子を生成する第1手段と、

上記受信メッセージに含まれるデジタル署名のうち、最新のものから順にチェック対象として選ばれたデジタル署名から、これと対応する復号鍵を用いて署名データを復号する第2手段と、

上記復号された署名データから抽出された文書圧縮子と、上記チェック対象文書から生成された文書圧縮子とが一致するか否かを検査する第3手段と、

上記復号された署名データがバージョン管理情報を含む場合、該バージョン管理情報と上記チェック対象文書とに基づいて、前バージョンの電子化文書を復元する第5手段とを有し、

上記前バージョンの電子化文書を新たなチェック対象文書として、上記第1手段～第4手段を動作させることを特徴とする請求項15に記載の電子化文書の処理システ

ム。

【請求項17】ネットワークから、電子化文書と、少なくとも1つのデジタル署名を含む文書付属情報とを有する通信メッセージを受信するための手段と、上記ネットワークから受信した前バージョンの電子化文書とそれに付されたデジタル署名との関係をチェックするための検査手段と、ユーザからの入力操作に応じて、上記前バージョンの電子化文書に部分的な変更または情報追加を行い、新バージョンの電子化文書を生成するための手段、上記新バージョンの電子化文書と所定の関係をもつ新たなデジタル署名を生成するための手段と、上記新バージョンの電子化文書と、前バージョンの電子化文書と共に受信した文書付属情報と、上記新たなデジタル署名と、上記バージョン管理情報とを含む通信メッセージを上記ネットワークに送信するための手段とを有し、上記デジタル署名が、上記新バージョンの電子化文書を圧縮処理して得られた第1の圧縮子と、上記ユーザの個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報を圧縮処理して得られた第2の圧縮子とからなる署名データを、上記ユーザの秘密鍵で暗号化処理することによって生成されることを特徴とする電子化文書の処理システム。

【請求項18】前記検査手段が、上記受信メッセージに含まれる電子化文書をチェック対象文書として、該チェック対象文書に所定の圧縮処理を施して文書圧縮子を生成する第1手段と、上記受信メッセージに含まれるデジタル署名のうち、最新のものから順にチェック対象として選ばれたデジタル署名から、これと対応する復号鍵を用いて署名データを復号する第2手段と、上記復号された署名データから抽出された第1の圧縮子と、上記チェック対象文書から生成された文書圧縮子とが一致するか否かを検査する第3手段と、上記復号された署名データが第2の圧縮子を含む場合、上記受信メッセージに含まれるバージョン管理情報の最新のものから順にチェック対象として選び、チェック対象となったバージョン管理情報に所定の圧縮処理を施して得られた管理情報圧縮子を生成する第4手段と、上記管理情報圧縮子と、上記復号された署名データから抽出された第2の圧縮子とが一致するか否かを検査するための第5手段と、上記復号された署名データが第2の圧縮子を含む場合、上記チェック対象となったバージョン管理情報と上記チェック対象文書とに基づいて、前バージョンの電子化文書を復元する第6手段とを有し、上記前バージョンの電子化文書を新たなチェック対象文書として、上記第1手段～第6手段を動作させることを

特徴とする請求項17に記載の電子化文書の処理システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、電子化文書処理システムに関し、更に詳しくは、電子化文書データに付されるデジタル署名の生成および認証のための技術に関する。

【0002】

10 【従来の技術】例えば、電子メールシステムを利用して、1つの文書を起案者から複数の関係者に順次に回覧し、各関係者に文書内容に対する承認を得る場合、承認した文書内容と承認者に署名との対応関係に、回覧の途中または後日に、不正な改ざんが加えられた否かを発見できるようにするため、文書データを圧縮して得たダイジェストデータ（ハッシュトータル）と承認者の個人データを暗号化して得られる「デジタル署名」の適用が知られている。

20 【0003】此種の電子化された文書データの正当性を確認するための技術は、例えば、「暗号と情報セキュリティ」、編者：辻井重男／笠原正雄、発行：昭晃堂のページ：127～147に記載の技術など、従来から種々の技術が提案されている。

【0004】図17に、デジタル署名を利用した電子化文書の認証方法の一例を示す。

30 【0005】10A～10Cはネットワークを介して相互に通信する機能をもつ端末装置であり、端末装置10Aの利用者（署名者A）が文書1301を起案し、上記文書1301に署名者Aのデジタル署名SAを付した形のメッセージを端末装置10Bに送信する。端末Bの利用者（署名者B）は、受信した文書1301の内容に同意すると、端末装置10Aから受信した文書1301とデジタル署名SAに自分のデジタル署名SBを追加した形のメッセージを、文書回覧ルートにある次の端末装置10Cに送信する。ここでは、端末装置10Cの利用者Cが、上記文書に付されたデジタル署名SA、SBの正当性を確認する場合の動作を示す。

40 【0006】端末装置10Aにおいて、デジタル署名SAは、次のようにして生成される。先ず、一方向の関数である圧縮関数1302aを用いて、文書データ1301の圧縮子（ハッシュトータル）を得る。得られた文書データの圧縮子と、キーボードから入力した署名者Aの個人情報（例えば、署名者Aの名前などのデータ）とで署名データ1303aを構成する。デジタル署名SA：1306aは、上記署名データ1303aを署名者Aの秘密鍵1304aを用いて暗号化する（暗号処理1305a）ことによって得られる。

50 【0007】端末装置10Bにおける署名者Bのデジタル署名SBも、上記署名者Aのデジタル署名SAと同様にして、圧縮関数1302bによって圧縮された文

書1301の圧縮子と、署名者Bの個人情報とで構成される署名データ1303bに、署名者Bの秘密鍵1304bを用いた暗号処理1305bを施すことによって得られる。

【0008】端末装置10Cにおけるデジタル署名1306a、1306bの正当性の確認は次のようにして行われる。まず、上記デジタル署名1306a、1306bに、それぞれ署名者A、Bの公開鍵1307a、1307bを用いた復号処理1308a、1308bを施すことによって、署名データ1303a、1303bを得る。この後、圧縮関数1302cを用いて、受信文書1301の圧縮子を生成し、これと署名データ1303a、1303bに含まれる文書の圧縮子とを比較する(検査関数1309a、1309b)。

【0009】なお、この方式では公開鍵暗号方式を使用しているため、デジタル署名は秘密鍵を知る本人だけにしか作れず、安全性を維持できる。

【0010】

【発明が解決しようとする課題】然るに、文書を複数の人に回覧し、各回覧先で文書内容を承認あるいは確認したことを示す署名を行う場合に、回覧途中で、既に誰かが署名済みの文書に対して、コメントの追加や誤字訂正など、文書内容の部分的変更が必要となる場合がある。また、文書中に予め部門毎の記入欄が設けてあり、複数の部門に回覧することによって完成される文書もある。

【0011】このように、回覧の途中で内容が変化する文書に対して、上述した従来のデジタル署名を適用すると、内容変更前のバージョンの文書に付されたデジタル署名を復号化して得られる文書の圧縮子と、最新バージョンの文書データから生成した圧縮子とが一致しなくなる。

【0012】このため、文書の最終的な確認者または回覧途中の署名者が、文書に付されたデジタル署名に対して上記端末Cで行った方法で認証操作した場合に、善意の基づく文書の修正あるいは更新であったにもかかわらず、文書または署名に不正があったことを示す判定結果が出されるという不都合が生ずる。

【0013】本発明の目的は、既にデジタル署名を伴っている文書データに対して善意による内容変更を許容できるようにしたデジタル署名の生成方法およびシステムを提供することにある。

【0014】本発明の他の目的は、それぞれバージョンの異なる文書内容と対応する複数のデジタル署名を伴った電子化文書の認証方法およびシステムを提供することにある。

【0015】本発明の他の目的は、デジタル署名を伴う電子化文書データを受信し、文書内容に追加あるいは部分的変更をした上で新たなデジタル署名を追加できるようにした電子化文書処理システムを提供することにある。

【0016】

【課題を解決するための手段】上記の目的を達成するため、本発明に係る電子化文書処理システムでは、ネットワークから受信した既に他の署名者による少なくとも1つのデジタル署名を伴う電子化文書に対して、ユーザが文書内容の追記または変更を行なった場合に、新バージョンの電子化文書を圧縮処理して生成した文書の圧縮子と、ユーザ(署名者)の個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とからなる署名データを用いて、上記ユーザのデジタル署名を生成する。上記デジタル署名は、例えば、公開鍵暗号化法において各ユーザに割り当てられた秘密鍵を用いて、上記署名データを暗号化することによって得られる。

【0017】上記デジタル署名は、ネットワークから受信した前バージョンの電子化文書に付されていた他の署名者のデジタル署名と共に、上記新バージョンの電子化文書に関係付けられ、文書回覧ルートの次の人に送信される。

【0018】本発明の電子化文書処理システムでは、回覧途中で何れかの署名者によってバージョンアップされた電子化文書を受信した場合でも、最後のデジタル署名から順に処理対象に選び、適宜、前バージョンの電子化文書への復元処理を実行しながら、デジタル署名と電子化文書との関係をチェックすることによって、各デジタル署名と電子化文書の正当性を認証することが可能となる。

【0019】

【作用】デジタル署名と電子化文書との関係チェックは、各デジタル署名をその署名者の公開鍵で復号化することによって署名データを復元し、該署名データから抽出された文書圧縮子と、実際に受信された電子化文書を圧縮処理して得た文書圧縮子とを比較することによって行われる。

【0020】本発明によれば、復元された署名データがバージョン管理情報を含む場合、これを用いて現在バージョンの電子化文書から1つ前のバージョンをもつ文書を復元できるため、全てのデジタル署名について、電子化文書との対応関係の確認が可能となる。

【0021】例えば、元の電子化文書が予め定義された複数の部分領域を有し、回覧の途中で、電子化文書中のこれらの部分領域の1つに文書データを追記することによって文書のバージョンアップがなされるようになっていいる場合、上記バージョン管理情報として、データが新たに追記された上記部分領域の1つを特定するための情報が適用される。

【0022】電子化文書中の任意の部分領域でデータの挿入または既存文書データの削除を行うことによって文書のバージョンアップがなされるようになっている場合、上記バージョン管理情報は、例えば、上記部分領域

を特定するための位置情報と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなる。

【0023】バージョン管理情報は、情報量が少ない場合は、これを署名データの1部に組込、暗号化されたデジタル署名の形で、回覧ルートの他の人（端末装置）に通知できる。バージョン管理情報の情報量が多い場合は、バージョン管理情報をそのまま電子化文書の付属情報の1部として、送信すればよい。

【0024】後者の場合、回覧途中におけるバージョン管理情報に対する不正な改変行為の有無を発見できるようにするために、例えば、バージョン管理情報を圧縮処理して得られた圧縮子を署名データに組み込み、これを暗号化処理してデジタル署名を生成するとよい。

【0025】このようにすると、電子化文書を受信した端末装置（電子化文書処理システム）では、デジタル署名を復号化して得られた署名データに含まれるバージョン管理情報の圧縮子と、電子化文書と共に受信したバージョン管理情報を圧縮して得た圧縮子とを照合することによって、上記バージョン管理情報が正当なものであることを確認した上で、該バージョン管理情報に基づいて、現在の電子化文書から1つ前のバージョンの電子化文書を復元することができる。

【0026】電子化文書に順次に付されるデジタル署名には、バージョン管理情報を伴ったものと、バージョン管理情報を伴わないものとが混在していてもよい。なぜなら、電子化文書を受信した端末装置においては、最新のデジタル署名およびバージョン管理情報から順に処理対象に選び、処理対象となったデジタル署名がバージョン管理情報またはその圧縮子を含む場合にのみ、現在処理対象としているバージョン管理情報を用いて、上述した1つ前のバージョンをもつ電子化文書の復元処理を実行すればよいからである。

【0027】

【実施例】図2は、本発明の一実施例であるデジタル署名機能を備えた複数の文書処理端末装置からなるメール通信システムの構成を示すブロック図である。図2において、10（10A、10B～10N）は、通信網12により相互に接続された端末装置であり、各端末装置10は、後述するように、文書の作成機能と、デジタル署名の生成および確認機能と、他の端末装置との間での通信機能をもつ。ここでは、デジタル署名付き電子化文書データ（以下、単に文書データという）が、予め指定された文書の回覧ルートに沿って、1つの端末装置から通信網12を介して他の端末装置に送信されるものとして説明するが、端末装置間の通信にメールサーバ20を介在させ、各端末がメールサーバ20をアクセスすることによって、文書データを回覧させるようにできること明らかである。

【0028】端末装置10は、図3に示すように、ディ

スプレイ1217と、キーボード1218と、各種のプログラムを格納するメモリ1205と、予め登録されたデータを格納するためのデータメモリ1206と、プログラム実行中に発生するデータを一時的に記憶するためのワークメモリ1207と、CPU（中央処理装置）1208と、通信制御部1209と、I/O制御部1210とを備えている。

【0029】上記プログラムメモリ1205には、複数のプログラムと、後述するデジタル署名の生成およびチェックのための複数の関数（モジュール）、具体的には、暗号処理のための関数1211、復号処理のための関数1212、データ圧縮処理のための関数（ハッシュ関数）1213、および認証データ検査のための関数1214を格納している。

【0030】データメモリ1206は、電子メールシステムを利用する予め登録された複数のユーザの公開鍵を記憶するエリア1209と、その端末を利用するユーザの秘密鍵を記憶するエリア1210とを有し、これらの秘密鍵と公開鍵は、それぞれユーザの識別番号IDを指定することによって読み出せるようになっている。

【0031】図1は、上記各端末10において行われるデジタル署名の生成方法の第1実施例を説明するための図である。ここでは、端末10Aにおいて利用者（署名者）Aが作成し、利用者Aのデジタル署名113Aと、次の利用者Bのデジタル署名113Bとが既に付された文書データ101を、端末10Cの利用者Cが受信し、上記文書の内容に部分的な変更を加えた後、利用者Cのデジタル署名113Cを付す手順を示す。

【0032】この実施例で、複数の利用者に順次に回覧される文書101は、内容変更を許されない固定的なデータ領域102と、回覧先でデータが追加される追加データ領域103とを有する。固定データ領域102は、最初の署名を行う文書起草者Aが生成した文書データを含む領域であり、最初の署名者A以外の者は、受信文書の固定データ領域102に含まれる文書内容を変更することが許されない。2番目以降の署名者が、受信した文書101に予め定義されている追加データ領域103に適宜データの書込みを行なうことにより、文書は情報量を増しながら、順次に回覧される。ここに示した例では、文書101の追加データ領域103は3つのサブ領域に分割され、前の署名Bが第1番目のサブ領域にデータを追加した状態にあり、署名者Cは、第2番目のサブ領域にデータを追加する。

【0033】端末10Cの利用者である署名者Cは、先ず、受信した文書データ101をディスプレイ1217の画面に出力した状態で、キーボード1218を操作して、文書データの追加処理104を行う。これにより、追加データ領域103の第2番目のサブ領域にデータが追加された、更新された文書データ105が生成される。本発明では、各署名者が、文書データを更新した上

でデジタル署名を行う場合に、自分がデータ修正した個所、この実施例ではデータを追加したサブ領域を特定する情報(サブ領域番号108)を、バージョン管理情報として、署名データ(認証データ)の1部に含めることを特徴とする。

【0034】文書データの更新が終わると、署名者Cは、更新された文書データ105に圧縮関数1213を用いて圧縮処理106を施し、文書圧縮子109を生成する。上記圧縮子109は、署名者Cの氏名等の個人情報110と、上述したサブ領域番号108と共に、署名データ107を構成する。上記署名データ107に対して、署名者Cに固有の秘密鍵111Cを用いて暗号処理112を施すことによって、文書データ105を署名者Cが承認したことを示すデジタル署名113Cが生成される。

【0035】署名者Cは、上記文書データ105と、文書データ101と共に受信した他の利用者のデジタル署名113A、113Bと、今回新たに生成した自分のデジタル署名113Cとを、図4に示す通信メッセージ100の形式で、次の署名者(または確認者)に送る。上記各デジタル署名113A~113Cと後述する公開鍵との対応関係を示すために、通信メッセージ100には、上記各デジタル署名113A~113Cと対をなして署名者の識別子114A~114Cが設定される。尚、図4では、簡単化のために、通信メッセージの送信先アドレス、発信元アドレス等の情報を含むヘッダ部を省略して示してある。

【0036】図5は、文書データを含む通信メッセージを受信した端末装置において、上述した署名動作の前処理として、あるいは閲覧された文書データの最終的な確認者による署名の正当性確認のために実行される、デジタル署名の確認処理を示す。

【0037】ここでは、デジタル署名113A~113Cを含む通信メッセージ100を受信した端末装置10Dの動作を例にして説明する。端末装置10Dでは、受信したメッセージから抽出した文書データ105に、圧縮関数1213を用いて、図1の処理106と同様の圧縮処理206を施し、文書の圧縮子109'を得る。次に、受信した通信メッセージ100から抽出したデジタル署名113A~113Cの内、最後のものから順にチェック対象署名とする。まず、デジタル署名113Cをチェック対象署名に選び、これと対をなす署名者Cの識別子114Cに基づいて、公開鍵記憶領域1216から署名者Cの公開鍵211Cを取りだし、この公開鍵211Cを用いて、デジタル署名113Cに復号処理212を施し、署名データ207を得る。

【0038】そして、上記圧縮処理206で得られた文書圧縮子109'と、署名データ207に含まれている文書圧縮子209とを検査処理214にかけ、これら2つの文書圧縮子が一致するかどうかを判定する。もし、

一致しない場合は、文書データ105、又はデジタル署名113Cに不正な改ざんが加えられているものと判断する。

【0039】上記検査処理214によって、2つの文書圧縮子109'と209との一致が確認された場合は、署名データ207に含まれるサブ領域番号208に基づいて、文書データ105中の署名者Cがデータを追加したサブ領域を特定し、このサブ領域に含まれるデータを削除する(文書復元処理204)。これによって、署名者Cの直前に署名者Bが承認した文書データ101が復元される。

【0040】上記文書データ101と、次のデジタル署名113Bを新たなチェック対象として、文書データ101の圧縮処理206と、デジタル署名113Bの復号処理212を行い、検査処理214、文書の復元処理204を行うと、追加データ領域203に追加データを含まない署名者Aが承認した文書データが復元される。従って、この文書データに上述した処理動作206、212、214を繰り返すことによって、デジタル署名113Aの正当性を確認することができる。以上のように、本実施例によれば、最終の署名者から順に、デジタル署名の検査と、データ追加サブ領域番号に基づく前バージョンの文書データ復元処理を繰り返すことによって、署名者全員についてのデジタル署名の正当性の確認を行うことが可能となる。

【0041】図6は、各端末装置10が備える上述した文書認証およびデジタル署名を実現するためのプログラムフローチャートを示す。このフローチャートでは、端末装置が、文書の閲覧ルートにおける任意順位、n番目の署名者に該当するものとして、扱われている。

【0042】前の閲覧者までのn-1個の署名が付された文書データ(通信メッセージ)を受信すると(ステップ302)、ディスプレイに文書データを表示し(ステップ303)、図7で詳述する署名確認処理ルーチンを実行する(ステップ304)。上記署名確認処理ルーチンでの確認結果は、パラメータのリターン値で示される。パラメータのリターン値をチェックし(ステップ305)、リターン値が「1」ならば、不正な改ざんがあったものと判断し、ステップ314で、文書データまたは署名が正当でないことを示すメッセージをディスプレイに表示して、このプログラムを終了する。

【0043】もし、リターン値が「0」ならば、上記文書データに付された全ての署名が正当であったと判断し、ステップ306で、署名が正当で合ったことを示すメッセージをディスプレイに表示し、利用者に氏名等の個人情報を入力させた後、文書への追加データの入力を許可する。ステップ307で、追加データ領域103における空き状態にあるi番目のサブ領域に、キーボードから入力されたコメント等の追加データを書き込み、これが終わると、ステップ308で、文書データに圧縮処

13

理を施して、文書圧縮子hを生成する。次に、上記ステップ306で入力された個人情報を変数Pに代入し（ステップ309）、変数Tにデータ追加サブ領域の番号iを代入し（ステップ310）、署名データSを生成する（ステップ311）。署名データは、 $S = (h \parallel P \parallel T)$ で表わされる。ここで、記号「 \parallel 」は、データの連結を意味している。

【0044】上記署名データSに対して、署名者の秘密鍵を用いた暗号処理を施し（ステップ312）、デジタル署名を生成する。そして、ステップ313で、今回更新された文書データ105と、今回受信したメッセージに含まれていた他の利用者のデジタル署名113A~113(n-1)と、新たに生成した署名113nを含む通信メッセージを編集し、次の閲覧者に送信する。

【0045】尚、文書の閲覧ルートは、一般には、文書101中の所定の領域に文字によって表示されるが、閲覧先となる各利用者の識別子とアドレスを通信メッセージの制御情報領域に予め設定しておき、1つの端末でデジタル署名の処理が終わると、自動的に次の人にメッ

ッセージが転送されるようにしてもよい。

【0046】図7は、署名確認処理ルーチン304の詳細を示すフロー図である。まず、チェック対象となる署名の総数を示す変数kに、今回受信したメッセージに含まれているデジタル署名の数「n-1」を代入する（ステップ321）。次に、k=0か否かを判定し（ステップ322）、k=0となっていれば、チェックすべき署名がないと判断し、ステップ323へ進んで、リターンコードに「0」を設定して、図6のプログラムにリターンする。もし、k≠0であれば、k番目のデ

ジタル署名に、その署名者の公開鍵を用いた復号処理を施し、署名データ $S = (h \parallel P \parallel T)$ を生成した後（ステップ324）、文書データに圧縮処理を施して圧縮子h'を生成する（ステップ325）。次に、上記復号化された署名データに含まれる文書圧縮子hと、圧縮子h'とを比較する（ステップ326）。

【0047】もし、 $h \neq h'$ ならば、不正な改ざんが行なわれていると判断し、ステップ329に進んで、リターンコードに「1」を設定し、図6のプログラムにリターンする。もし、 $h = h'$ ならば、正当な署名であると判断し、上記復号化された署名データに含まれる位置情報Tに基づいて、文書の追加データ領域のT番目のサブ領域に書かれたデータを削除した後（ステップ327）、変数kの値から1を引き（ステップ328）、判定ステップ322に戻る。

【0048】なお、このルーチンでは、ステップ327を繰り返すことによって、文書データが順次に前のバージョンに戻っていくが、次の署名者に送信すべき最新の文書データそのものは、別の記憶エリアに保存されており、このルーチンを実行することによって閲覧すべき文

14

書データが損なわれることはない。

【0049】本実施例によれば、各署名者は閲覧されてきた文書にコメント等の付加データを追加することができる。また、このようなデータの追加によって、デジタル署名の対象となる文書が閲覧途中で変形されても、本発明によれば、各デジタル署名と対応するバージョンの文書データを復元できるため、正当な署名を誤って不当な署名と誤診するおそれはない。

【0050】図8は、本発明によるデジタル署名の生成方法の第2の実施例を示す。この例では、署名者Bは、文書の起案者Aから受信した文書データ401の任意の領域において文書内容に変更を加え（文書変更処理402）、更新された文書データ403に対してデジタル署名を行う。署名者Bが受信文書に対して行った変更（データ追加、データの置換あるいは削除）の内訳は、図10で説明するバージョン管理テーブル（文書変更／更新管理テーブル）412に記録され、更新された文書データと共に、次の署名者に送信される。

【0051】デジタル署名は、次のようにして行われる。更新された文書データ403に圧縮処理404を施し、文書圧縮子407を生成する。また、バージョン管理テーブル412に圧縮処理413を施し、バージョン管理テーブル412Bの圧縮子406を生成する。署名データ405は、これらの圧縮子406、407と、署名者Bの氏名等の個人情報408とからなる。上記署名データ405に対して、署名者Bの秘密鍵409Bを用いた暗号処理410を施し、デジタル署名411Bを生成する。

【0052】更新された文書データ403と、バージョン管理テーブル412Bと、デジタル署名411Bは、それ以前のデジタル署名411Aとともに、図9の示すような通信メッセージ400の形式で、次の署名者（または確認者）に送信される。なお、受信した文書の内容の一部が、前の何れかの署名者Nによって既に更新されている場合、後の署名者Mによって新たに生成されたバージョン管理テーブル412Mは、既に存在するバージョン管理テーブル412Nに続く形で、通信フレームに挿入される。

【0053】バージョン管理テーブル412は、図10に示すように、データ変更が施された領域毎に生成される複数のレコード505、506、……からなる。各レコードは、データ変更の種類を示すコードを記憶するためのフィールド501と、文書中におけるデータ変更が施された部分領域の先頭位置を示すアドレスを記憶するためのフィールド502と、文書変更処理402で上記領域に新たに挿入されたデータのサイズを記憶するための503と、文書変更処理402で上記領域から削除されたデータを記憶するためのフィールド504とを含む。

【0054】フィールド501に設定されるコードの値

と処理内容との関係は、次のようになっている。

「1」：データの追加、「2」：データの置き換え、
「3」：データの削除。

【0055】図10に示した例において、例えば、レコード505は、受信した文書中のアドレス「279120」から部分領域に存在していた旧データ「u j i 8…8 y l」を長さ「3200」キャラクタの新たなデータに置き換えたことを意味する。上記新たなデータは、更新された文書403に存在している。レコード506は、受信文書中のアドレス「891236」から始まる部分領域に長さ「458」キャラクタのデータが挿入されたことを意味し、レコード507は、アドレス「114031」から始まる部分領域にあったデータ「k h t…450 j」が削除されたことを意味している。

【0056】図11は、上述したバージョン管理テーブル412を伴う文書データを受信した端末装置10Cで行われるデジタル署名の正当性確認の手順を示す。まず、受信メッセージから抽出した文書データ403に圧縮処理604を施すことによって、文書の圧縮子407'を生成する。次に、受信メッセージから抽出したデジタル署名411Bに対して、署名者Bの公開鍵609Bを鍵として復号処理610を施し、署名データ605を生成する。上記圧縮処理604で得た文書の圧縮子407'と署名データ605に含まれる文書の圧縮子607とを比較し（検査処理612）、2つの文書圧縮子が一致するかどうかを判定する。もし、これらが一致しない場合は、文書データ403またはデジタル署名411Bに不正な改ざんが加えられているものと判断する。

【0057】上記2つの文書圧縮子の一致が確認された場合は、受信メッセージから抽出した署名者Bのバージョン管理テーブル412Bに圧縮処理614を施し、テーブル圧縮子406'を生成する。得られたテーブル圧縮子406と、署名データ605に含まれているテーブル圧縮子606とを比較し（検査処理615）、これらの圧縮子が一致するかどうかを判定する。もし、これらが一致しないときは、バージョン管理テーブル412Bまたはデジタル署名411Bに不正な改ざんが加えられたものと判断する。

【0058】上記2つのテーブル圧縮子の一致が確認された場合は、バージョン管理テーブル412Bの各レコードの内容に基づいて、文書データ403に復元処理602を施し、署名者Aが承認したバージョンの文書データ401を得る。

【0059】上記復元処理602では、バージョン管理テーブル613の各レコードに示されたコード501に従って、追加された部分データの文書データ403からの削除（コードが「1」または「2」の場合）と、削除されたデータ504の文書データ403への挿入（コードが「2」または「3」の場合）とが行なわれる。

【0060】このようにして復元された文書データ40

1と、受信メッセージから抽出された署名者Aのデジタル署名411Aを対象として、上述した処理を繰り返すことによって、デジタル署名411Aの正当性チェックすることができる。

【0061】以上の如く、本実施例によれば、最終の署名者から順に、デジタル署名の正当性チェックと、前バージョンの文書データの復元処理を繰り返すことによって、回覧の途中で文書の任意の部分で内容更新がなされた場合でも、全ての署名者のデジタル署名の正当性を確認することができる。

【0062】図12は、図8に示したデジタル署名の生成方法の変形例を示す。この実施例では、文書の起草者は、文書の圧縮子と個人情報とからなる署名データを暗号処理してデジタル署名を生成し、2番目以降の署名者は、更新管理テーブル4の圧縮子406と、署名者の個人情報408とで署名データ405'を構成し、文書の圧縮子を含まない署名データ405'に対して署名者Bの秘密鍵409Bを用いた暗号処理410を施すことによって、デジタル署名411B'を生成するようにしたものである。

【0063】このデジタル署名の作成方法は、例えば、回覧先の各署名者毎に文書中の特定のコメント領域が割り当てられ、各署名者が文書の一部を必ず更新するような構造をもつ文書に対して有効となる。

【0064】図13は、図12に示した方法で生成されたデジタル署名をもつ文書データを受信した端末装置10Cで行われる2番目以降のデジタル署名の正当性確認の手順を示す。文書データの圧縮子の生成と検査（図11における処理604と612）が省略されている点を除いて、図11で説明した動作と同様の動作が行われている。最初の署名者に関しては、図11に示したように、文書を圧縮処理して得た圧縮子と、署名データから抽出した文書圧縮子との比較によって、その正当性をチェックする。

【0065】本実施例によれば、文書の圧縮子に関する検査を1部省略できるため、認証動作を高速化することができる。

【0066】図14は、バージョン管理テーブル412の変形例900を示す。ここに示したバージョン管理テーブル900は、複数の署名者に共用されるもので、各レコード907~911は、署名者の個人識別子を記憶するフィールド901と、更新処理の種類を示すコードを記憶するためのフィールド902と、文書中におけるデータ変更が施された部分領域の先頭位置を示すアドレスを記憶するためのフィールド903と、文書変更処理402で上記領域に新たに挿入されたデータのサイズを記憶するための904と、文書変更処理402で上記領域から削除されたデータを記憶するためのフィールド905と、デジタル署名を記憶するためのフィールド906とからなる。

【0067】最初の署名者である文書データの起案者は、レコード907に示すように、個人識別子と、文書更新がないことを示すコード「0」と、デジタル署名とをテーブルに登録する。

【0068】受信した文書データに部分的な変更を加えた署名者は、修正箇所毎にレコードを生成し、各レコードに個人識別子分と、図10で説明したのと同様の定義に従ってバージョン管理情報(902~905)を登録する。複数の部分領域に対してデータ修正を施した署名者は、最後のレコードのフィールド906にデジタル署名を登録する。文書の起案者以外の署名者で、受信した文書データに変更を加えなかった者は、例えばレコード910に示すように、署名者の個人識別情報と、コード「0」と、デジタル署名とを登録する。

【0069】上記バージョン管理テーブル形式を採用した場合、各端末が送受信する通信メッセージは、最新の文書データと、それに続くバージョン管理テーブルとからなるフレームフォーマットとなる。

【0070】図15は、図1で説明したデジタル署名生成方法の変形例を示す。この例では、文書の圧縮処理1006で処理対象とする文書領域を2つに分け、文書105の固定データ領域102に含まれるデータの圧縮子1010と、追加データ領域103に含まれるデータの圧縮子1009とを別個に生成する。これらの圧縮子1009、1010と、個人情報1011と、サブ領域番号108とで署名データ1007を構成し、これの署名データに対して、署名者Cの秘密鍵111Cを用いた暗号処理112を施し、デジタル署名1013Cを作成する。

【0071】図16は、上述したデジタル署名1013Cを伴う文書データを受信した端末装置10Dで行われる署名の確認手順を示す。端末装置10Dは、受信メッセージから抽出した文書データ105に圧縮処理2006を施し、固定データ領域102に含まれるデータの圧縮子1010'と、追加データ領域103に含まれるデータの圧縮子1009'とを生成する。また、上記受信メッセージから抽出されたデジタル署名1013Cに、署名者Cの公開鍵211Cを用いて復号処理212を施すことによって署名データ2007を得る。

【0072】デジタル署名1013Cの正当性は、固定データ領域102に関するデータ圧縮子1010'と署名データ2007に含まれるデータ圧縮子2010との一致、および、追加データ領域103に関するデータ圧縮子1009'と署名データ2007に含まれるデータ圧縮子2009との一致をそれぞれ検査処理2014でチェックすることによって行う。

【0073】本実施例によれば、デジタル署名に異常が検出された時、文書データの改ざん箇所が、固定データ領域102と追加データ領域103の何れにあるかを特定できる利点がある。

【0074】なお、上述した全てのデジタル署名の生成方法は、文書データの種別(テキスト、図形、音声、画像、またはそれらを合成したもの)に依らず適用可能である。

【0075】

【発明の効果】以上の説明から明らかなように、本発明によれば、バージョン管理情報を用いたことによって、現在の文書データから順次に1つずつ前のバージョンの文書データを復元できるため、回覧の途中で、文書データの1部に不正でないデータの追加、変更などの処理が加わった場合でも、各署名者のデジタル署名と、その前提となる文書データとの対応関係を間違いなく認証することができる。

【図面の簡単な説明】

【図1】本発明によるデジタル署名生成手順の第1の実施例を説明するための図。

【図2】本発明を適用する複数の端末からなる電子メールシステムの全体構成を示す図。

【図3】端末装置の構成を示すブロック図。

【図4】第1実施例における通信メッセージの構成を示す図。

【図5】第1の実施例におけるデジタル署名の確認手順を説明するための図。

【図6】デジタル署名の確認と生成を行うためのプログラムフローチャート。

【図7】図6における署名確認処理ルーチン304の詳細を示すフローチャート。

【図8】本発明によるデジタル署名生成手順の第2の実施例を説明するための図。

【図9】第2実施例における通信メッセージの構成を示す図。

【図10】バージョン管理テーブルの構造を示す図。

【図11】第2の実施例におけるデジタル署名の確認手順を説明するための図。

【図12】本発明によるデジタル署名作成手順の第3の実施例を説明するための図。

【図13】第3の実施例におけるデジタル署名の確認手順を説明するための図。

【図14】バージョン管理テーブルの変形例を示す図。

【図15】本発明のデジタル署名生成手順の第4の実施例を説明するための図。

【図16】第4の実施例におけるデジタル署名の確認手順を説明するための図。

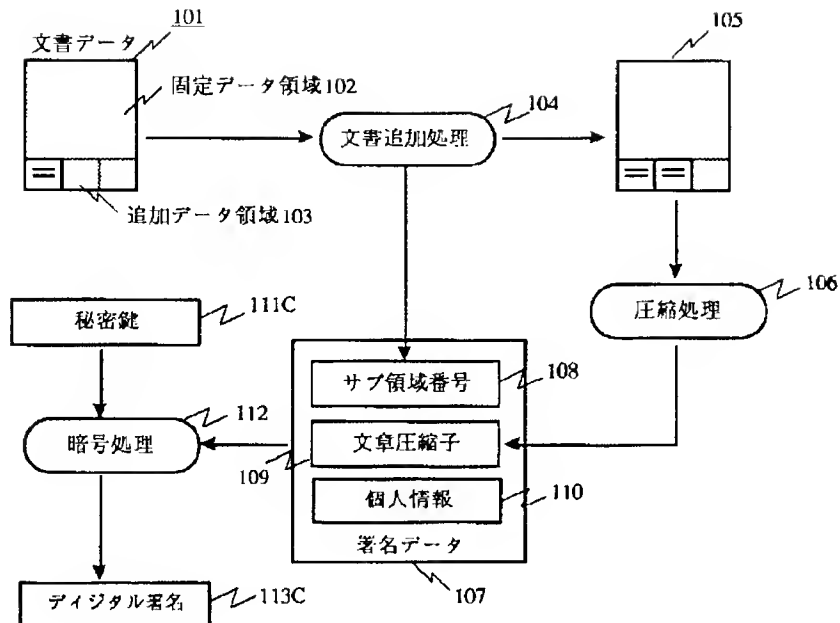
【図17】従来のデジタル署名の処理方法を説明するための図。

【符号の説明】

101…元の文書データ、105…新バージョンの文書データ、107…署名データ、108…バージョン管理情報、111…秘密鍵、113…デジタル署名、211…公開鍵、207…デジタル署名。

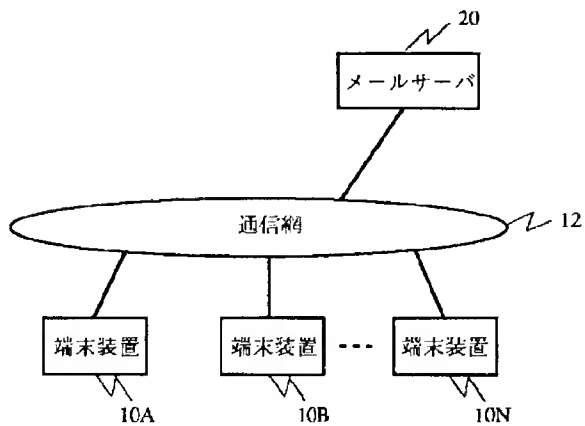
【図1】

図 1



【図2】

図 2



【図10】

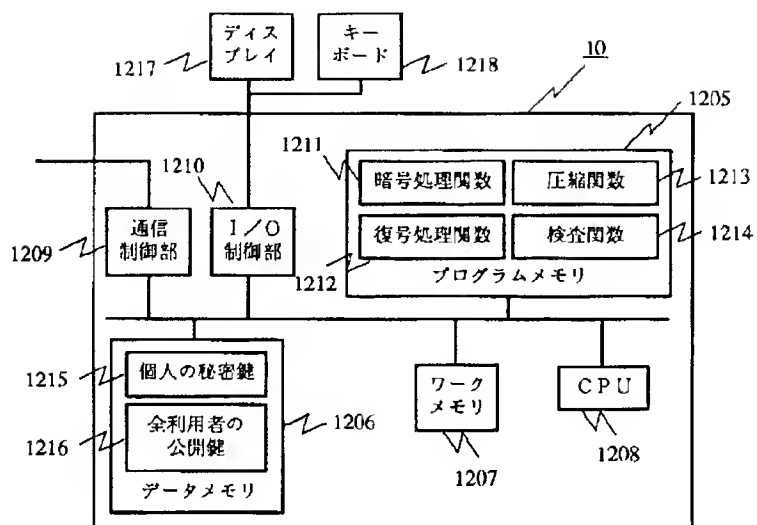
図 10

	501 コード	502 アドレス	503 サイズ	504 データ
505	2	279120	3200	ujr843qhlivha...wef8yha8yl
506	1	891236	458	—
507	3	114031	—	khtp0u65poj...retu9iyw45oj
	⋮	⋮	⋮	⋮

バージョン管理テーブル 412

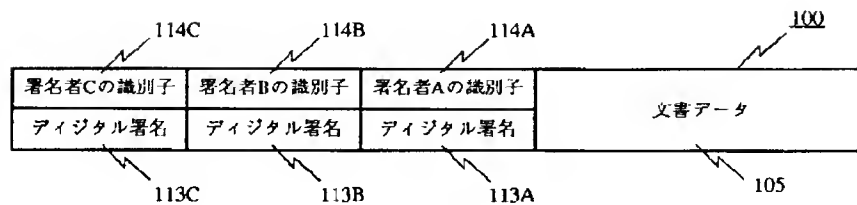
【図3】

図 3



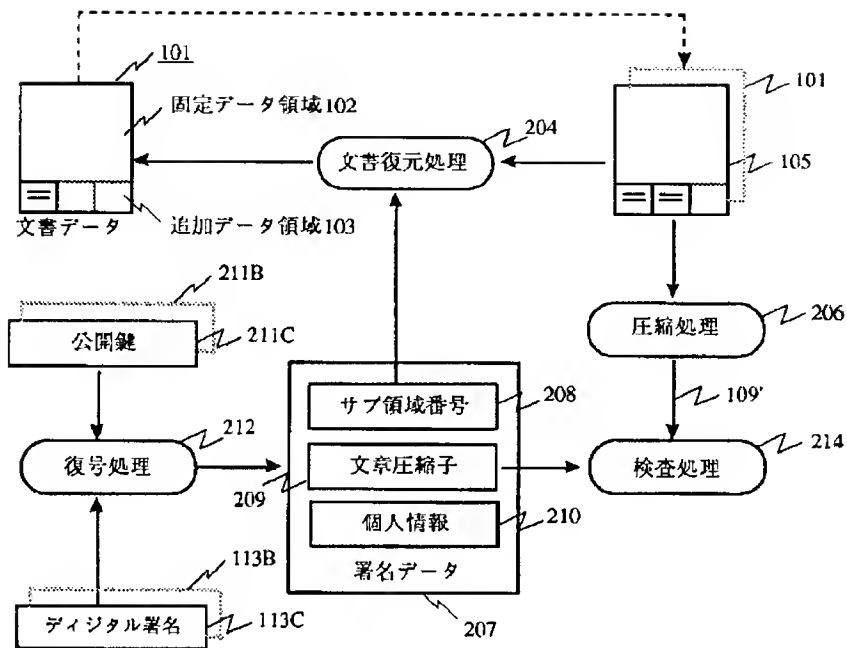
【図4】

図 4



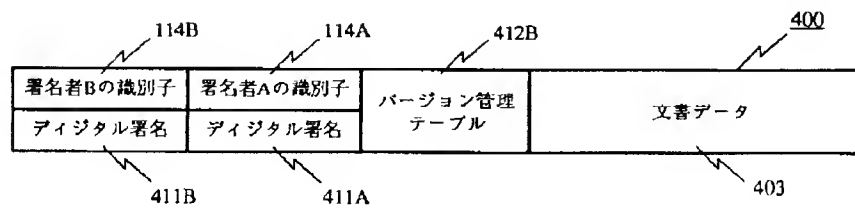
【図5】

図 5



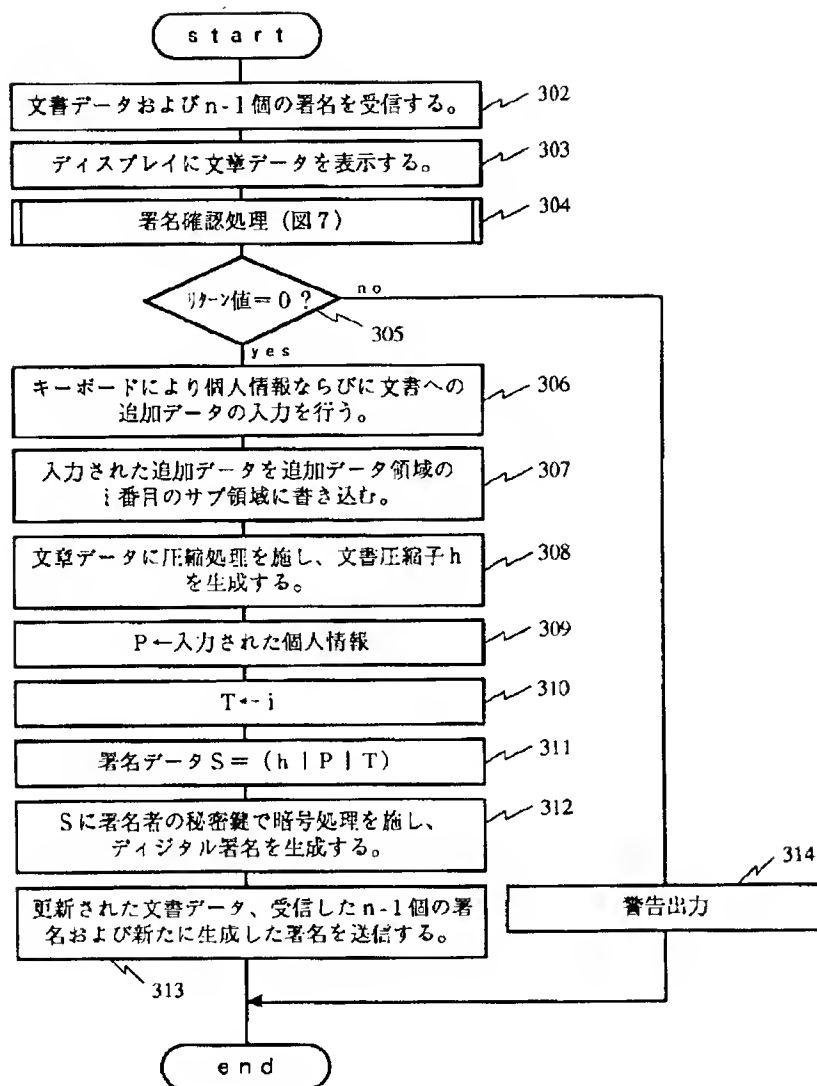
【図9】

図 9



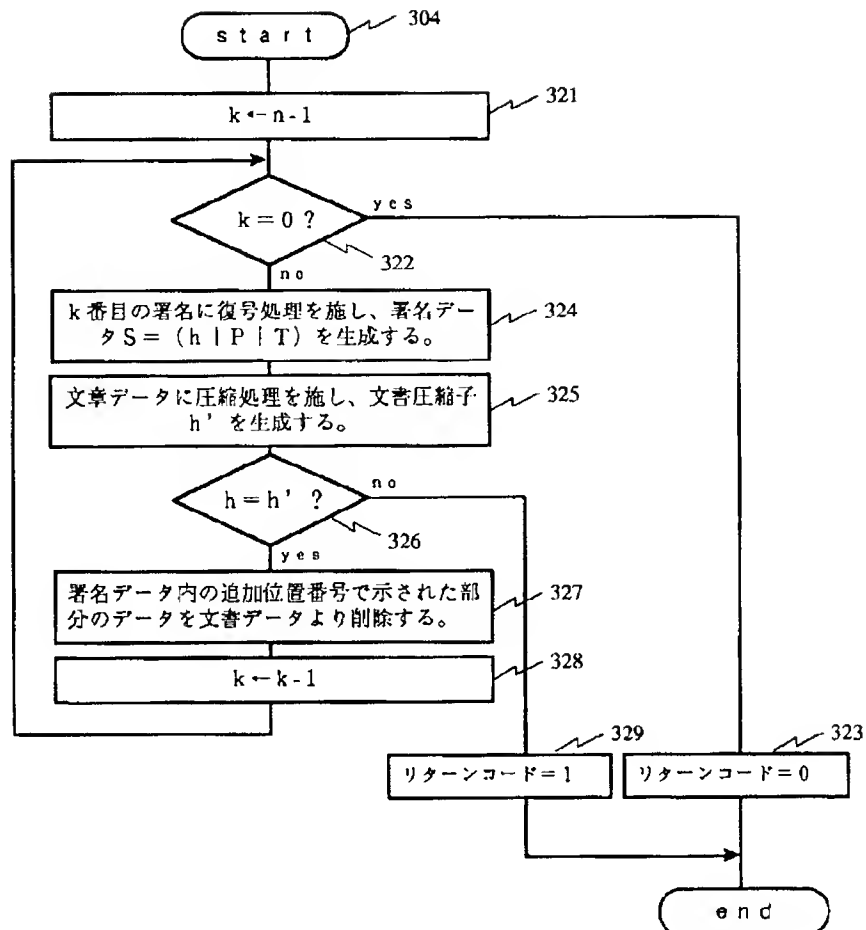
【図6】

図 6



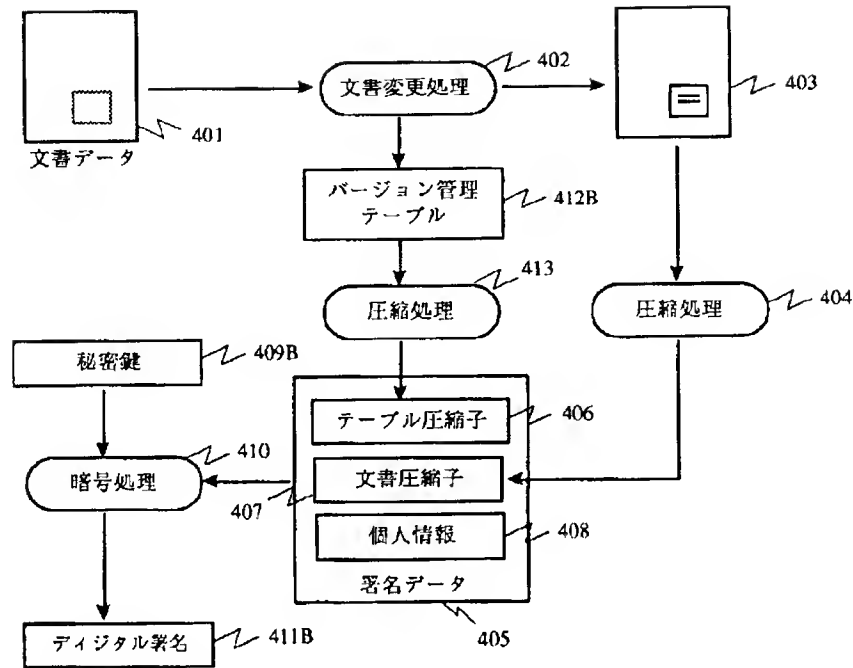
【図7】

図 7



【図8】

図 8



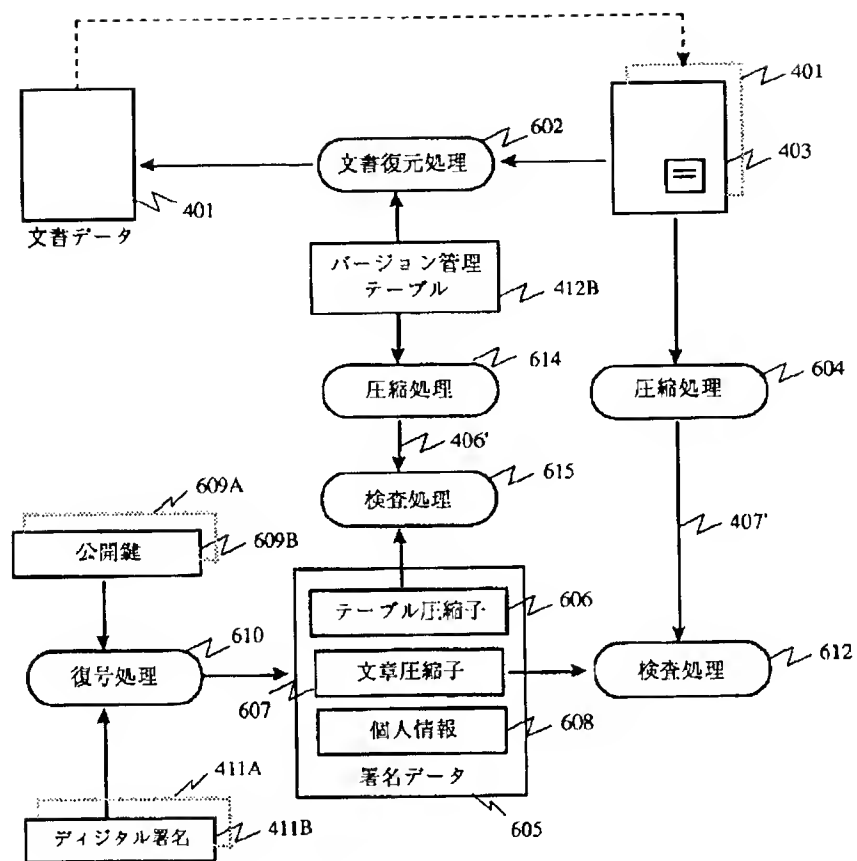
【図14】

図 14

	901	902	903	904	905	906
	入力ID	コード	アドレス	サイズ	データ	デジタル署名
907	A	0	—	—	—	1101...010
908	B	2	279120	3200	uj;8:3qhl-yha0yl	—
909	B	1	891236	458	—	1000...110
910	C	0	—	—	—	0100...110
911	D	3	114031	—	khAp0u63...rlyw45oj	0111...010
	⋮	⋮	⋮	⋮	⋮	⋮

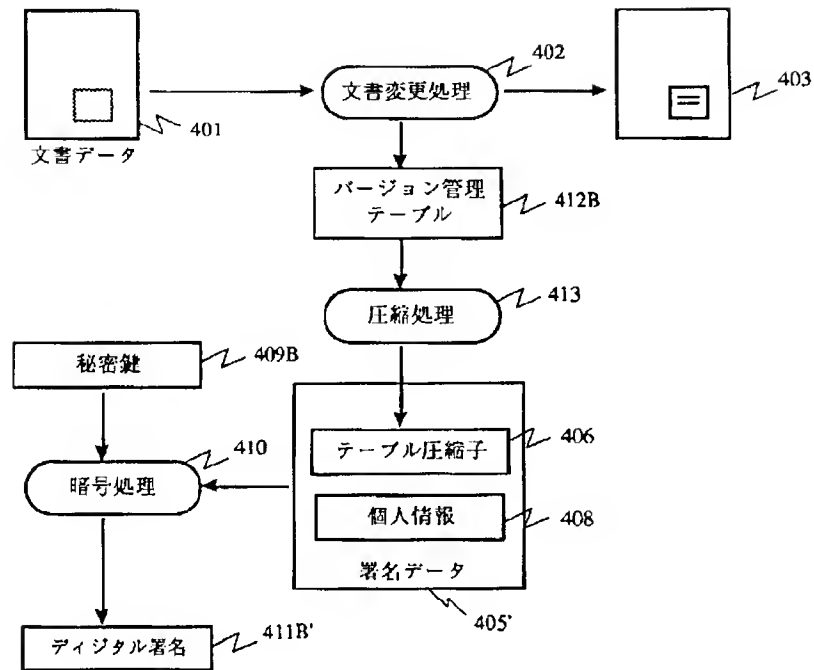
バージョン管理テーブル 902

☒ 11



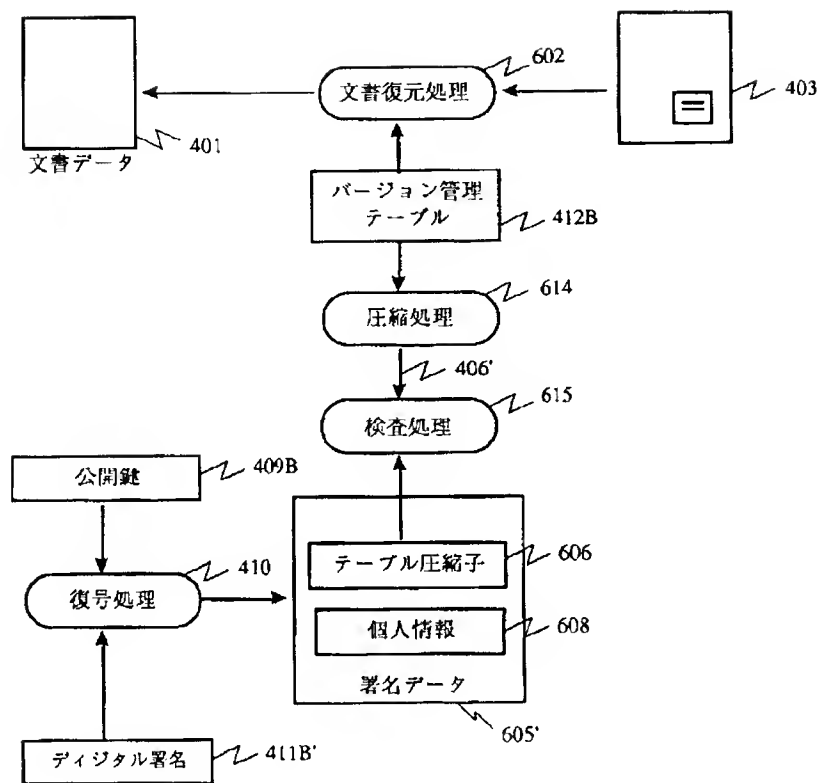
【図12】

図 12



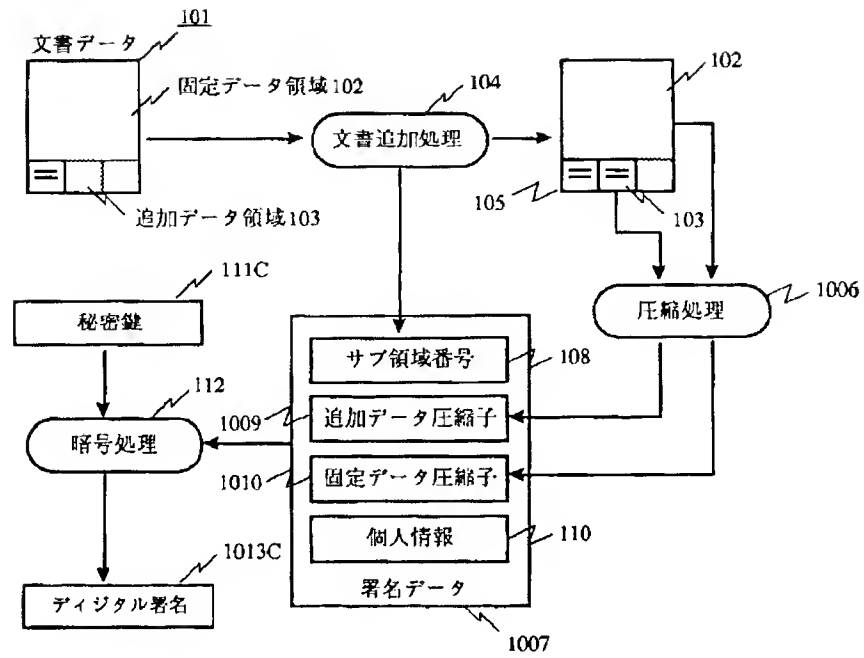
【図13】

図 13



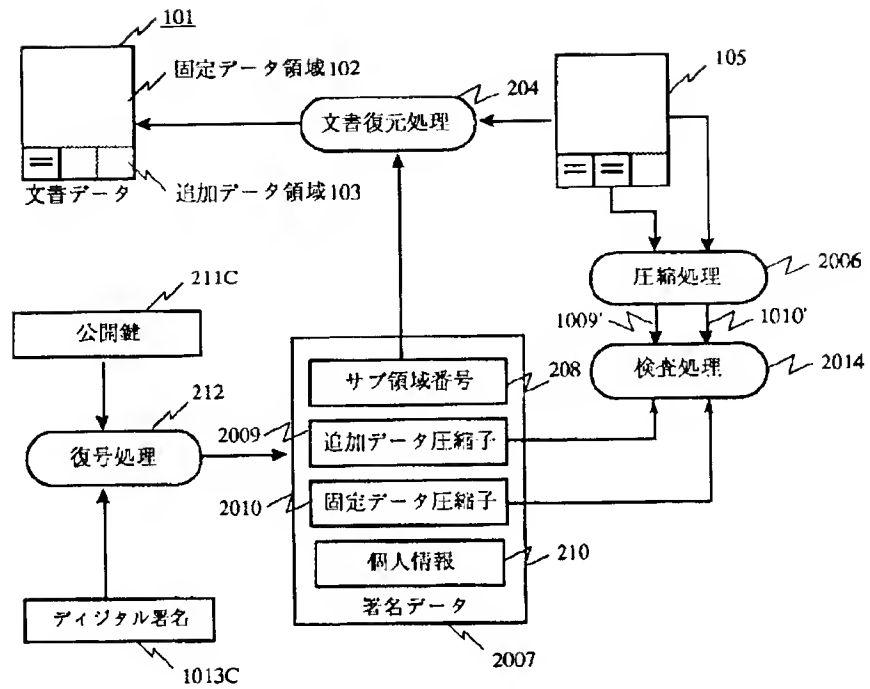
【図15】

図 15



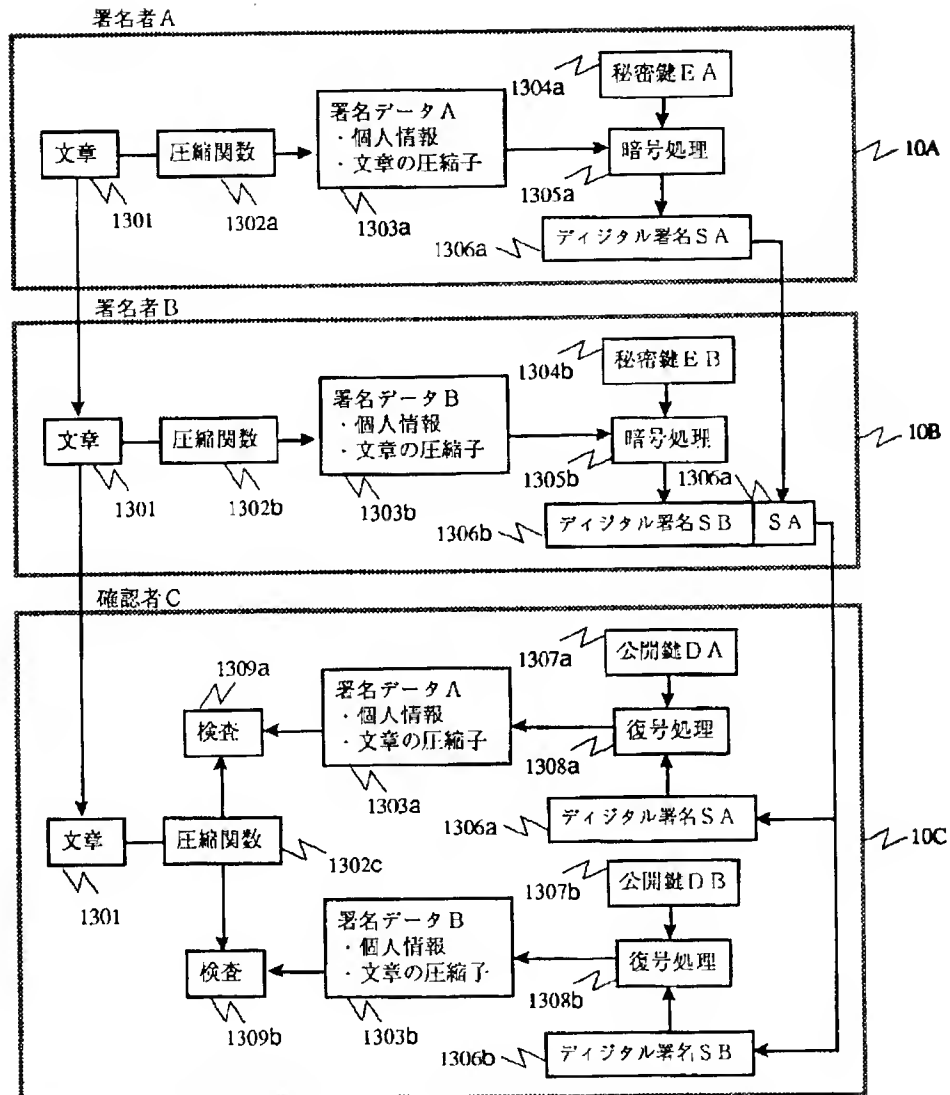
【図16】

図 16



【図17】

図 17



フロントページの続き

(72)発明者 洲崎 誠一
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 前澤 裕行
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 小泉 忍
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

【公報種別】特許法第17条の2の規定による補正の掲載
【部門区分】第7部門第3区分
【発行日】平成13年4月6日(2001.4.6)

【公開番号】特開平6-224896
【公開日】平成6年8月12日(1994.8.12)
【年通号数】公開特許公報6-2249
【出願番号】特願平5-303773
【国際特許分類第7版】

H04L 9/00

9/10

9/12

G09C 1/00

【F1】

H04L 9/00 Z

G09C 1/00

【手続補正書】

【提出日】平成12年4月5日(2000.4.5)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正内容】

【発明の名称】デジタル署名の生成方法

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】少なくとも1つのデジタル署名が関係付けられている前バージョンの電子化文書について、文書データの追記または変更を行なって新バージョンの電子化文書を作成し、上記新バージョンの電子化文書を圧縮処理して文書の圧縮子を生成し、上記文書圧縮子と、署名者の個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とを含む署名データを暗号化処理して、新たなデジタル署名を生成し、上記新バージョンの電子化文書に、上記前バージョンの電子化文書に係付けられていたデジタル署名と上記新たなデジタル署名とを関係付けることを特徴とするデジタル署名の生成方法。

【請求項2】前記署名データの暗号化処理が、公開鍵暗

号化法において前記署名者に割り当てられた秘密鍵を用いて行われることを特徴とする請求項1に記載のデジタル署名の生成方法。

【請求項3】前バージョンの電子化文書が、データを追記するために用意された予め定義された複数の部分領域を有し、前記新バージョンの電子化文書が、前バージョンの電子化文書中の上記部分領域の1つに文書データを新たに追記することによって生成され、前記バージョン管理情報は、文書データが新たに追記された上記部分領域の1つを特定するための情報からなることを特徴とする請求項1に記載のデジタル署名の生成方法。

【請求項4】前記文書圧縮子が、前記新バージョンの電子化文書中の前記複数の部分領域に含まれる文書データを圧縮処理して得られる第1の圧縮子と、前記新バージョンの電子化文書中のその他の領域に含まれる文書データを圧縮処理して得られる第2の圧縮子とからなることを特徴とする請求項3に記載のデジタル署名の生成方法。

【請求項5】前記新バージョンの電子化文書が、前バージョンの電子化文書中の少なくとも1つの部分領域での新文書データの挿入または既存文書データの削除を行うことによって生成され、前記バージョン管理情報が、上記部分領域の位置と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなることを特徴とする請求項1に記載のデジタル署名の生成方法。